UNITED STATES ARMY MATERIEL COMMAND
HARRY DIAMOND LABORATORIES
WASHINGTON 25, D.C.

(16) 1P222901A207,
~~5B91,21,17500~~
HDL Proj 16100

(17) TM-64-4

(11) 30 January 1964,
(19) 41 p.

(6) AN INTRODUCTION TO PSEUDO-NOISE MODULATION,

(10) J. P. Chandler

FOR THE COMMANDER:
Approved by

Clyde D. Hardin
Clyde D. Hardin
Chief, Laboratory 100

CONTENTS

ABSTRACT

The chief purpose of this report is to provide an introduction to pseudo-noise modulation functions and to describe those properties that make their use in radar systems desirable. Because of the interests of these laboratories, characteristics applicable to fuzes are emphasized.

The applicability and usefulness of various pseudo-noise modulation functions in radar systems is discussed. The use of the m-sequence in a complete radar system is described, and an extensive bibliography of other applications to radar systems is also given. A short section containing classified information on jamming of pseudo-noise modulated radars, with bibliography, is issued as a supplement to this report.

This report is essentially a survey, and the body of the report therefore contains little new material. However, the three appendices, on mesh relations for sequences with two-level autocorrelation, on the shift-and-add relations, and on filter integration of m-sequences, present material that to the author's knowledge is original.

1. INTRODUCTION

During the past decade, a new class of modulation functions has been developed and applied to communication, guidance, and radar systems. Called pseudo-noise or pseudo-random, these functions are digital in nature. In the application of these functions, a transmitted signal having a small number of modulation states, usually two, is employed. The signal is then alternated between the states as prescribed by the digital code.

Compared with conventional pulse or CW radar, radar systems using these functions may exhibit new, and, in many ways, better performance characteristics such as

(a) large average- to peak-power ratio
(b) unambiguous measurement of range to large ranges
(c) unambiguous measurement of velocity (Doppler frequency) to high velocities
(d) fine range resolution
(e) fine velocity resolution
(f) resistance to both sophisticated and power jamming
(g) a signal difficult for an enemy to detect because of its peak-free, noise-like spectrum.

Ordinary CW radar is completely satisfactory with respect to average power and measurement of velocity but neither resolves nor measures target range satisfactorily. On the other hand, a pulse radar using short pulses and a low duty cycle eliminates the ranging problem but sacrifices average power and the unambiguous

measurement of velocity. The velocity measurement becomes ambiguous because many short pulses must be used, and Doppler must be determined through a pulse-to-pulse phase-shift measurement instead of through an intrapulse frequency measurement. In the pulse-to-pulse method, the phase-shift measurement is unambiguous only from $-\pi$ to $+\pi$; hence, the magnitude of the largest unambiguous Doppler frequency is one half of the pulse repetition frequency. The result is that only low frequencies can be measured unambiguously.

That digital modulation functions can mitigate the disadvantages of pulse radar to some extent may be illustrated as follows. Assume that the waveform may be transmitted in one of two modulation states, M1 or M2, which may be phase states, frequency states, amplitude states, or, in the limit, off-on states (M2 = M0). For a system using phase modulation, the more usual case, the waveform in state M1 is illustrated in figure 1(a); in states M1 and M2, in figure 1(b). In this case, M1 and M2 differ by 180 deg in phase.

The unambiguous range of the pulse radar may now be increased by transmitting the successive pulses in either state M1 or M2 as prescribed by a binary sequence, either specified or random. If the sequence is periodic with a period of L digits, the unambiguous range has been extended by a factor of L. Unfortunately, the integration time has been extended similarly. If the sequence is aperiodic, a more complicated situation arises, to be treated later.

If, instead of desiring to increase the unambiguous range, we desire to increase the range resolution, and, if the change of state can be accomplished sufficiently rapidly, then we may code each pulse with a binary sequence (fig. 1(c)). In this case, the range resolution and bandwidth are both increased by a factor L.

Alternately, if the average power is to be increased, pulses modulated as in figure 1(b) may be concatenated as in figure 1(d). The limit of such a concatenation is modulated CW. In addition, it can be shown that the velocity resolution is best, in a certain sense, if angle-modulated CW is used (ref 16, p. 24).

If immunity to countermeasure is prime, then an aperiodic sequence or one of long period and complicated structure might be employed. With such a sequence, it will be difficult for a jammer to produce an "advanced" waveform; i.e., one designed to deceive the receiver by falsely registering as a near target, because the sequence is theoretically or practically unpredictable. In this case, of course, the receiver would be much more complicated.

Although it would be desirable to hide the modulated signal in a peak-free, noise-like spectrum, it is usually not possible to do so in a radar system, because the transmitted power is so large as to be easily recognized even with substantial spectrum spreading. The

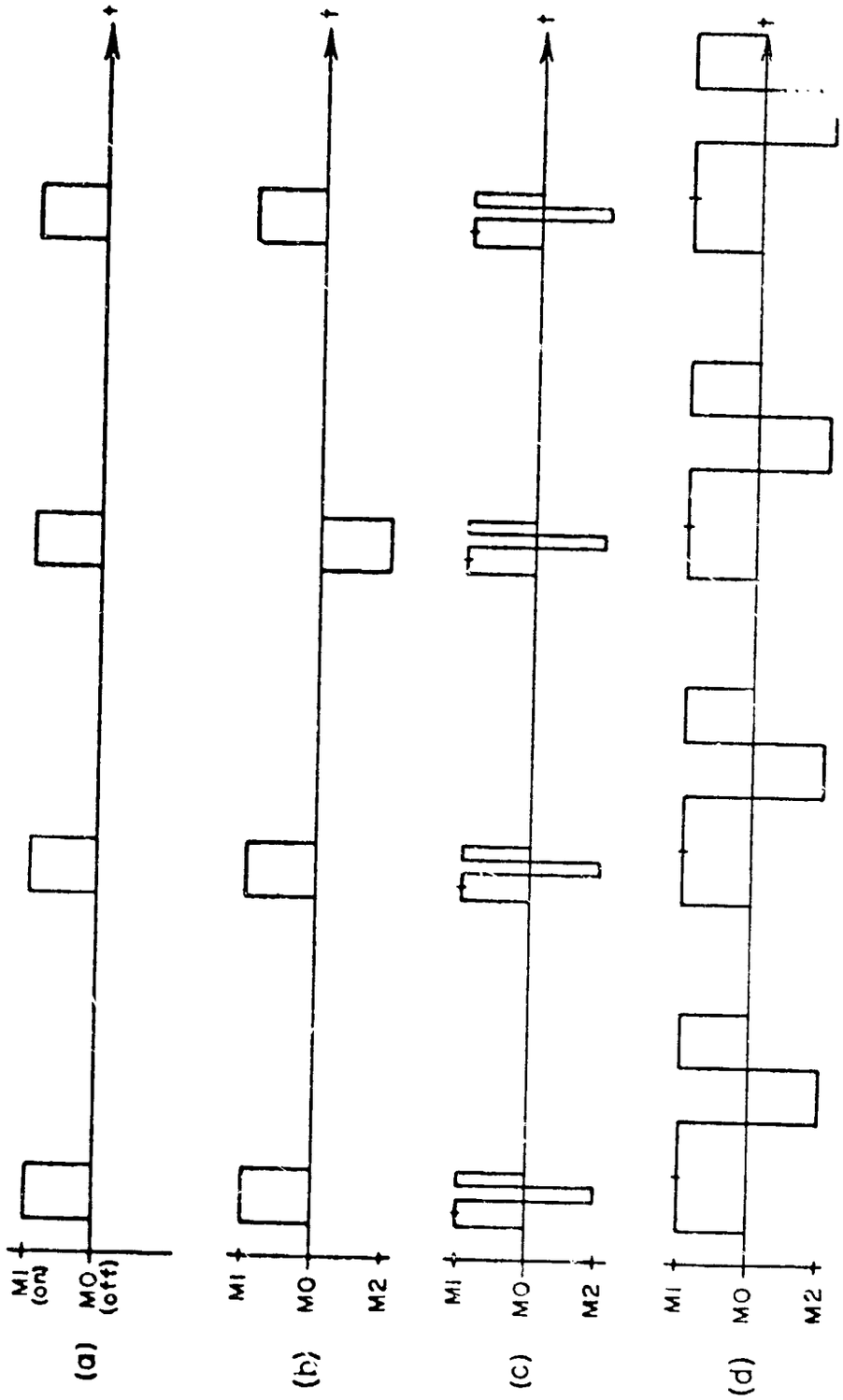


Figure 1. Improvement of pulse radar characteristics.

technique may be useful, however, in a secret communications system where power may be minimized. Modulation of the message by a binary sequence is then a form of scrambling that spreads the spectrum (fig. 2(a)). If the receiver can remove the binary modulation through knowledge of the sequence, the received spectrum (message) is collapsed (fig. 2(b)). At the same time, any CW present, which may be CW jamming, is spread, while uncorrelated noise is not collapsed. The message may then be separated by a narrow-band filter.

This illustration of the application of various modulation functions to pulse radar has thus shown how certain disadvantages of conventional pulse radar may be alternatively alleviated, but not without obtaining certain other disadvantages. The illustration implies, however, that by proper choice of the modulation function, it may be possible to obtain a number of advantages simultaneously without obtaining serious disadvantages. The objective of this report is to examine the various modulation functions with this in mind, to weight their relative advantages, and ideally, to arrive at a best modulation function.

2. THE RADAR RECEIVER AND TRANSMITTED WAVEFORM

The most that can be required of a radar receiver is that it compute a probability density for a target at each range associated with return delays τ and each velocity associated with Doppler frequencies ϕ.[1] Assuming a single point-target and Gaussian noise, it has been shown (ref 2,3,4) that no receiver can extract more information from the received signal than a correlation (matched-filter) receiver. For a transmitted waveform w(t), the delayed, Doppler-shifted return is

$$r(t) = w(t - \tau)\, e^{2\pi i \phi t} + n(t) \qquad (1)$$

where n(t) represents additive noise. A correlation receiver is one that computes the envelope

$$\text{env } C(\tau,\phi) = |\Gamma(\tau,\phi)|$$

$$= \left|\frac{1}{2}\int_I r^*(t)\, w(t - \tau)\, e^{2\pi i \phi t}\, dt\right| \qquad (2)$$

[1] If the radar system becomes ambiguous in τ and/or ϕ, no attempt is made to resolve these ambiguities. Therefore, sufficiently strong returns from the ambiguous (τ,ϕ) region will be falsely interpreted as returns from the unambiguous region and their probabilities so computed.

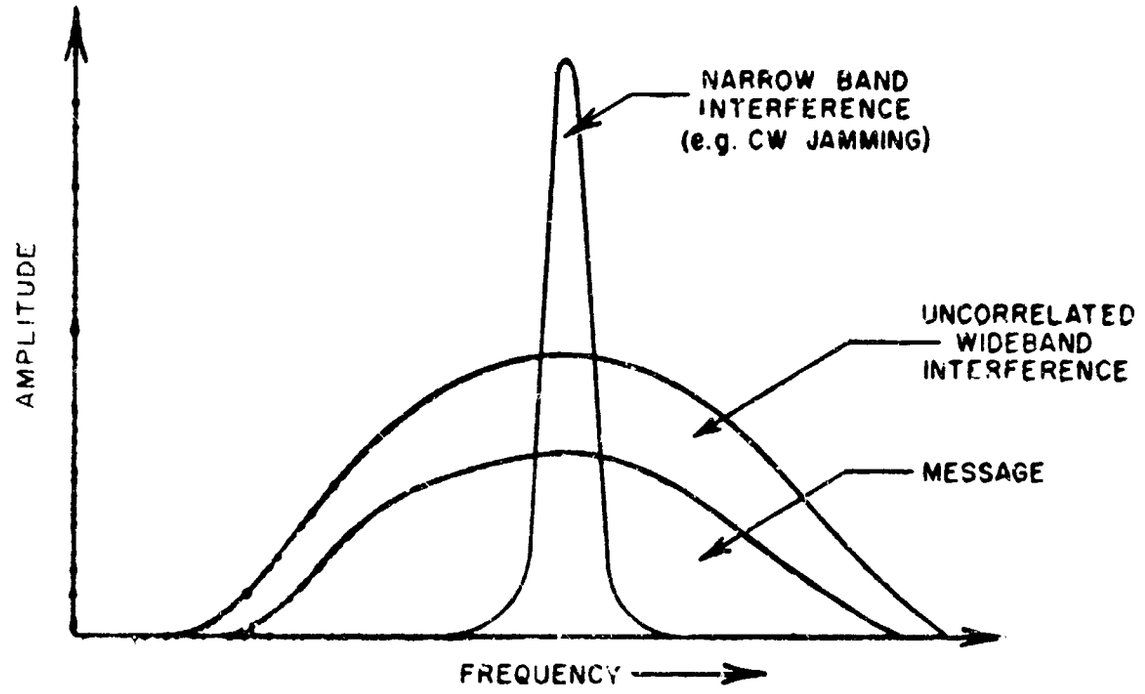


Figure 2(a). Spectrum received.

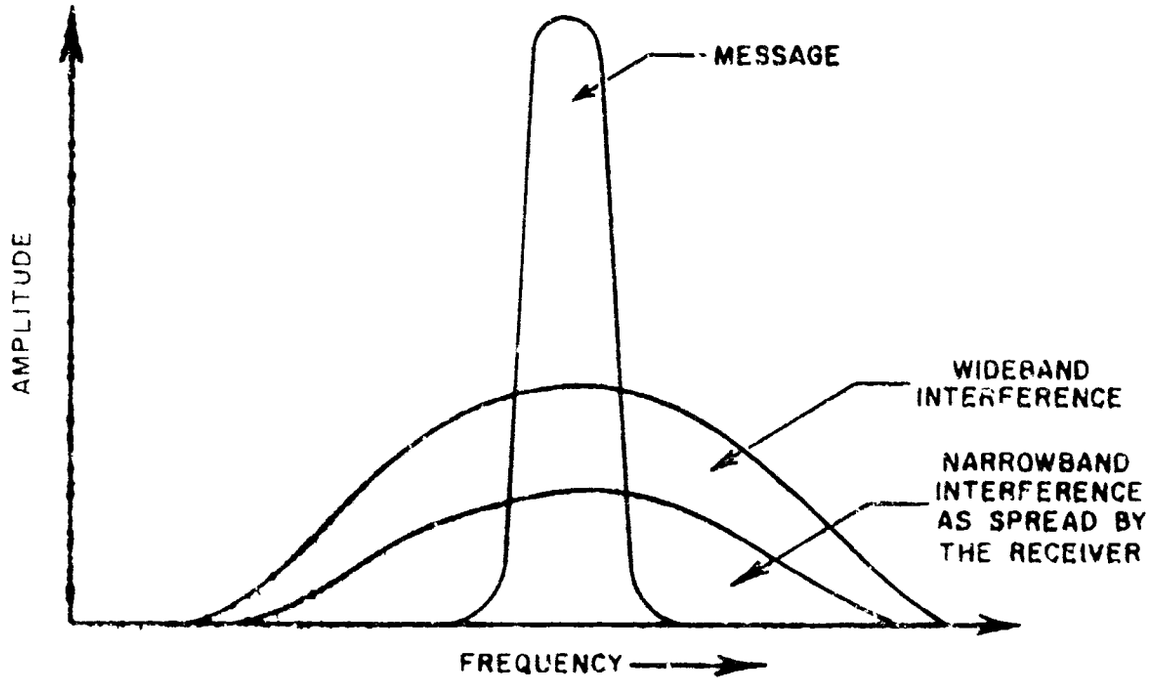


Figure 2(b). Spectrum after code demodulation.

where I is the interval of integration, i.e., the conjugated signal is multiplied by a delayed, frequency-shifted reference, integrated, and the envelope taken (to discard rapid fluctuations in $C(\tau,\phi)$ that carry no information). Various receivers of this type have been designed[1] and are described in the references.

Although a correlation receiver extracts all available information from a given signal, some transmitted signals have more suitable characteristics than others. The function that measures the suitability of a waveform in this respect is the signal component of $\Gamma(\tau,\phi)$ which, after a change of origin, is Woodward's famous ambiguity function

$$X(\tau,\phi) = \int_I w(t)\, w^*(t-\tau)\, e^{-2\pi i\phi t}\, dt \qquad (3)$$

For most radar purposes, a good waveform w(t) is one for which the envelope $|X(\tau,\phi)|$ of $X(\tau,\phi)$ has a sharp peak at the origin and is small elsewhere.

We expect to use a carrier modulated by a low-pass modulation function:

$$w(t) = x(t)\, e^{2\pi i\phi_c t} \qquad (4)$$

Then,

$$|X(t,\phi) = \left|\int x(t)\, x^*(t-\tau)\, e^{-2\pi i\phi t}\, dt\right| \qquad (5)$$

and so the pertinent ambiguity function is that of the modulation waveform.

Along the τ axis, $|X|$ is just the envelope of the autocorrelation function of $x(t)$:

$$|X(\tau,0)| = \left|\int x(t)\, x^*(t-\tau)\, dt\right| \qquad (6)$$

[1] This kind of correlation receiver is to be distinguished from another class of distance-measuring correlation systems that does not delay the reference signal, and that essentially takes the magnitude of env $C(\tau,\phi)$ at the origin as a measure of the nearness of the peak of env $C(\tau,\phi)$ to the origin. Such a system is described by B.M Horton, "Noise-Modulated Distance Measuring Systems," IRE Proceedings, Vol 47, 1959, pp 821-828.

For certain important modulations, the ambiguity function is much better (i.e., smaller) along the τ axis than elsewhere in the plane. The modulation period (and the integration interval) is made shorter than the shortest expected Doppler period in order to guarantee that correlation of the received signal with a delayed but not frequency-shifted signal will give a small off peak value.

The ambiguity functions of common waveforms such as pulsed sine waves and "chirp" signals have been calculated and found to be far from optimal (ref 3, 4, 30). Except for a few modulations as yet unexploited in systems (ref 7), the study of better modulation functions has been restricted to time-quantized "telegraph signals" like those in figure 1. Henceforth we will consider only functions of this type: the modulator chooses among a fixed, finite number of modulation states at multiples of a basic time interval. The modulation waveform will be represented by a sequence of complex numbers, each modulation state being symbolized by one member of the sequence.

3. BINARY DIGITAL MODULATION OF PULSE RADAR

To begin with, we will investigate the simplest case of binary modulation of pulse radar, where there are two modulation states. It is sometimes convenient to take these as

$$a_k = +1 \text{ or } -1 \tag{7}$$

and at other times as

$$b_k = 0 \text{ or } 1 \tag{8}$$

Generally, these will be associated in the order shown above; i.e.,

$$a_k = 1 - 2b_k \tag{9}$$

on those occasions when a change of variable is performed. If these sequences of a_k or b_k are associated directly with the modulation waveform via

$$x(t) = a_k \quad \text{or} \quad x(t) = b_k \tag{10}$$

$$kt_o \leq t \leq (k+1)t_o$$

then, the modulations are, respectively, 0 or 180-deg digital phase modulation, or on-off digital amplitude modulation. When discussing the mathematical properties of binary sequences, however, the actual form of modulation will be disregarded during the analysis.

and the above change of variable made whenever it is mathematically convenient. Although the only operation between a_k's will be ordinary multiplication, the b_k's will be either multiplied or subjected to "addition modulo two," whichever happens to be convenient to the calculation or proof at hand. The latter operation is defined so that it corresponds to multiplication of the a_k's and is symbolized by $\oplus$:

×	+	−
+	+	−
−	−	+

Multiplication of ± 1

$\oplus$	0	1
0	0	1
1	1	0

Addition modulo two of 0,1

that is,

$$0 \oplus 1 = 1 = 1 \oplus 0 \tag{11}$$

$$0 \oplus 0 = 0 = 1 \oplus 1 \tag{12}$$

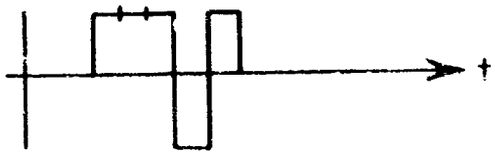
The first class of binary coded waveforms that we will examine is exemplified by figure 1(c). In these, a coded pulse is followed by an off-time longer than the pulse. An investigation of the entire ambiguity function will not be made, since it happens that the autocorrelation function itself (which is the zero-velocity cross section of the ambiguity function) is not one particularly suitable with long sequences.

3.1 Coded Words and Phase-Coded Pulses

If the two modulation states M1 and M2 differ only in phase, and in that by 180 deg, the coded pulse is most naturally represented by a finite sequence, "word" of a_k's. The autocorrelation function of a coded word is given by

$$C_a(\tau) = \sum_{k=1}^{L-\tau} a_k \, a_{k+\tau} \tag{13}$$

where τ is a discrete variable, $\tau = \cdots, -2, -1, 0, 1, 2, \cdots$; L is the word length, and the autocorrelation is unnormalized; e.g., for the coded word (+1, +1, +1, -1, +1), the pulse waveform is



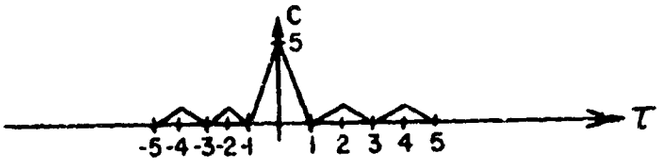
and $a_1 = a_2 = a_3 = a_5 = +1$; $a_4 = -1$. Then $C_a(1)$ is computed from the partial overlap

$$\begin{array}{ccccc} + & + & + & - & + \\ & + & + & + & - & + \end{array}$$

and is equal to

$$C_a(1) = 1 + 1 - 1 - 1 = 0 \tag{14}$$

The autocorrelation function for this pulse is



and furthermore, this is representative of the class of coded words with the best autocorrelation function:

$$C_a(\tau) = \begin{cases} 0 \text{ or } \pm 1 \ , & \tau = \pm 1, \pm 2, \cdots, \pm(L-1) \\ N \ , & \tau = 0 \end{cases} \tag{15}$$

Unfortunately, the longest known such "perfect" word is only 13 digits long. There are no longer ones of odd length (ref 33). The existence of longer perfect words of even length hinges on the unsolved problem of the existence of long "perfect" periodic sequences, which will be mentioned later. Their existence is considered unlikely. Some of the known perfect words are (ref 1)

L	Perfect Word
2	+ -
3	+ + -
4	+ + + -, + + - +
5	+ + + - +
7	+ + + - - + -
11	+ + + - - - + - - + -

There has been some experimental investigation of "nearly perfect" words: $|C_a(\tau)| = 2$ or 3 off-peak.

3.2 Coded Vowels and On-Off Coded Pulses

If, on the other hand, the two states M1 and M2(=M0) are on and off, the coded pulse is best represented by a finite sequence, or "vowel" of b_k's. Such pulses have been used in the Venus ranging experiment (ref 1, 46, 55). On-off coding was used because the return was not phase-coherent.

The autocorrelation function for a coded vowel is

$$C_b(\tau) = \sum_{k=1}^{L-\tau} b_k b_{k+\tau} \tag{16}$$

i.e., an overlap product analogous to word correlation. The perfect autocorrelation in this case is defined as

$$C(\tau) = \begin{cases} \dfrac{N+1}{2} & , \tau = 0 \\ 0 \text{ or } 1, & \tau \neq 0 \end{cases} \tag{17}$$

An example of a perfect vowel is 1100101[1], few are known.

4. BINARY CODES FOR CW

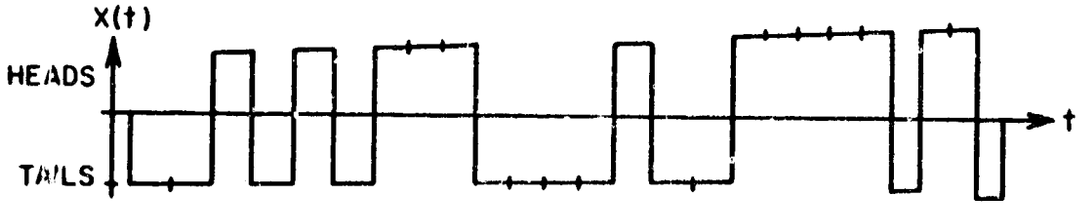
The case of continuous transmission remains; we now treat digital coded CW (the conventional but somewhat anomalous term) and in the next section restrict the codes to binary sequences. Most of the systems built so far employ 0- to 180- deg phase modulation (PM), although a few use AM or FM. PM will be assumed in most cases, and accordingly, the sequences will correspond directly to the modulation when written in terms of the a_k. Most sequences considered will be periodic, but first, an aperiodic sequence with certain advantages will be treated.

4.1 The Fair Coin Sequence

If the sequence a_k is chosen by flipping a fair coin, it has the advantage of being unpredictable to the jammer. There is no possible way to jam it intelligently, and recourse must be made to brute-force techniques. Since the sequence is aperiodic, no range ambiguities are built in.

A typical section of a telegraphic modulation function obtained by actual coin-flipping appears as

[1] It is to be noted that the association previously given in eq (9) (+1 → 0) and (-1 → +1) does not carry perfect vowels into perfect words.



The normalized autocorrelation function of the modulation is

$$C(\tau) = \lim_{T \to \infty} \frac{1}{2T} \int_{-T}^{T} x(t)\, x(t+\tau)\, dt \tag{18}$$

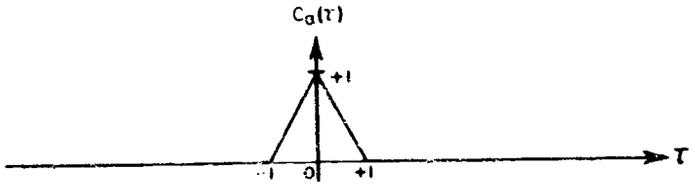
The autocorrelation function is zero except for $\tau = 0$ because there are equal numbers of agreements and disagreements between a_k and $a_{k+\tau}$. The former contribute +1 to $C(\tau)$; and the latter, -1. In fact, an alternate definition of the normalized autocorrelation function of any a_k sequence is

$$C_a(\tau) = \frac{A-D}{A+D} \tag{19}$$

where A is the number of agreements during the period of correlation, and D, the number of disagreements. In the limit of equation (18), then, it is clear that

$$C_a(\tau) = \begin{cases} 1 & , \quad \tau = 0 \\ 0 & , \quad |\tau| \geq 1 \end{cases} \tag{20}$$

for the random sequence



Now, this is the same as the autocorrelation of a single rectangular pulse.[1] And according to the Wiener-Khintchine Theorem, the Fourier transform of the autocorrelation function is just the power spectrum. Hence, the power spectrum of the modulation waveform x(t) is exactly the same as that of the pulse, which is the familiar $(\frac{\sin^2 x}{x^2})$.

The above autocorrelation function is not practical for radar applications in that by its definition, it requires an

[1] Although we have considered $C_a(\tau)$ only for integral τ, the definition (18) may be employed to develop the continuous curve shown.

infinite correlation time (ref 31). If the correlator integrates for only L digits, the autocorrelation is represented as in figure 3; for a given τ, the value of the finite sum could lie anywhere between the dotted lines with probability 1/2 it will lie within the shaded region if L is large (ref 6); its expectation is the heavy solid line, i.e., the autocorrelation function previously computed for the limit $L \to \infty$.

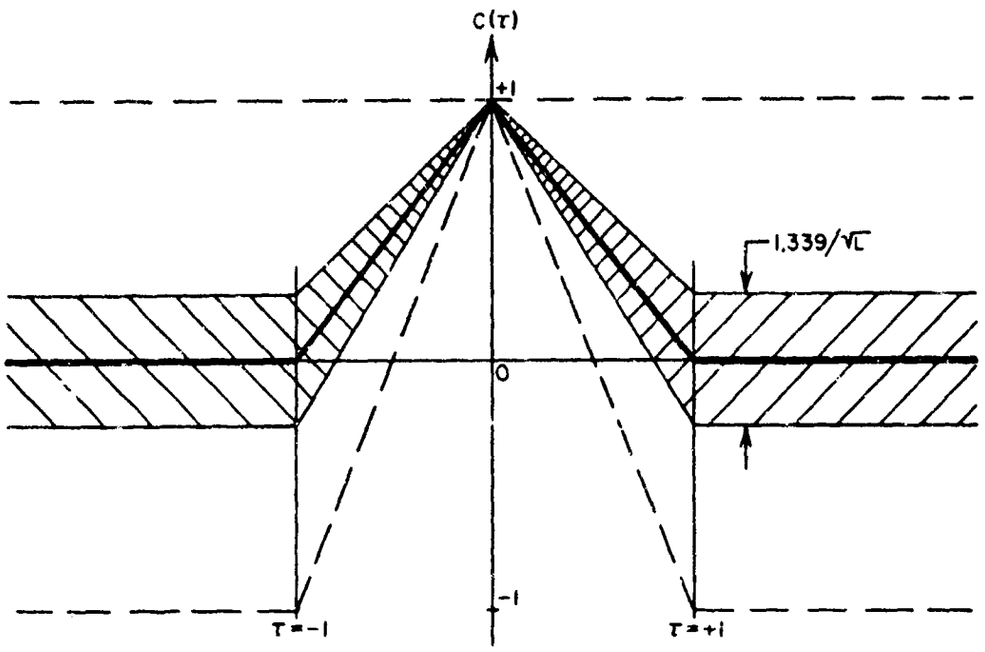


Figure 3. Finite integration-time autocorrelation for the fair-coin sequence.

Lytle (ref 32) has analyzed the more restricted case of randomly chosen periodic sequences.

4.2 Pseudo-Random Sequences

There exist preassigned (and in fact periodic) sequences having autocorrelation properties nearly as good as those of random sequences without the disadvantage of random fluctuations in their

correlation. They exhibit properties close to those that random sequences have only on the average. For this reason, they are called "super-random" or, more commonly, "pseudo-random."[1]

The following postulates obtaining pseudo-randomness have been often used in various combinations:

P1) In each period, the number of +1's is nearly equal to the number of -1's.

P2) In each period, half of the runs (groups of consecutive digits of the same kind) are of length one, one quarter are of length two, one eighth of length three, $\cdots 2^{-m}$ of length m; etc. For a finite period, this must end somewhere, viz., at least at the time $2^{-m} = 1/L$.

P3 For a period of length 2^n, every n-tuple appears once per period.

P4) The ambiguity function of the corresponding modulation should have a sharp peak at the origin, and be small and uniform to some specified degree elsewhere. In particular, the autocorrelation shall be two level:

$$C_a(\tau) = \sum_{k=1}^{L} a_k \, a_{k+\tau} = \begin{cases} L, & \tau = 0 \\ M, & \tau \neq 0 \end{cases} \qquad (21)$$

This autocorrelation is cyclic, unlike the pulse case previously considered; e.g., for the sequence (- - - + + - +), $C_a(2)$ is computed from the comparison of the sequence with its cyclically shifted self:

$$|- - - + + - + \,|\, - - - + + - +|$$

$$|- - - + + - +|$$

where | represents an arbitrary division into periods. Here,

$$C_a(2) = +1 \; -1 \; -1 \; -1 \; +1 \; +1 \; -1$$
$$= -1$$

[1] Generally speaking, a sequence is called "random" if the method of generation has no known properties (e.g., natural laws or preferred initial conditions) that would cause departures from randomness. A sequence is called "pseudo-random" if, regardless of its method of generation, it satisfies some particular set of criteria derived from the expectation values of a random sequence. As a result, a pseudo-random sequence usually appears more random than almost all random sequences of the same length.

and it can be verified that this particular sequence satisfies P4 but not P3:

$$C_a(\tau) = \begin{cases} 7, & \tau = 0 \pmod 7 \\ -1, & \tau \not\equiv 0 \pmod 7 \end{cases} \tag{23}$$

Sequences satisfying P3 are called de Bruijn sequences (ref 9, 10, 13, 23). They satisfy P1 and P2 but do not satisfy P4 if $n > 1$, as will be shown later. Adding one + to the above example forms a de Bruijn sequence of degree $n = 3$:

$$- - - + + + - +$$

P3 is now satisfied but P4 is not: $C_a(3) = -4$.

A de Bruijn sequence of arbitrary degree n can be formed by the following rule: let (a_1 to a_n) be (-) and continue the sequence writing a (+) whenever it does not complete an n-tuple appearing earlier in the sequence (ref 9). Thus for $n = 4$, this algorithm yields

$$- - - - + + + + - + + - - + - +$$

It is not possible in general to form a sequence satisfying P4 from a de Bruijn sequence by omitting the last element.

4.3 Sequences with Two-Level Autocorrelation

Only P4 is of direct interest for modulation sequences. The requirement that $C_a(\tau)$ be two-level has certain consequences, a number of which will be stated in this section in order to give the reader a familiarity with this class of sequence.

Consequence I—First of all, it is obvious that for any binary sequence, the unnormalized autocorrelation

$$C_a(\tau) = \sum_{k=1}^{L} a_k a_{k+\tau} = A - D \tag{24}$$

(or in fact any form of complete pairing, cyclic or not) consists of L terms each of which is (+1) or (-1), and hence,

$$C_a(\tau) \equiv L \pmod 2 \text{ for all } \tau. \tag{25}$$

But the stronger statement is true for autocorrelation or any complete pairing of binary sequences that

$$C_a(\tau) \equiv L \pmod 4 \text{ for all } \tau \tag{26}$$

This can be seen from a simple example:

If any group of Republicans and Democrats is paired off in any fashion against another group of the same size and political constitution, an even number of political arguments will ensue, equally divided between Republicans versus Democrats and Democrats versus Republicans.

Proof: Let the number of ordered pairs of each of the four kinds be symbolized in an obvious way: N_{DR} is the number of Democrat-versus-Republican pairings, etc. The number of Democrats in each group is

$$N_{DD} + N_{DR} = N_{DD} + N_{RD} \tag{27}$$

Hence, the number of disagreements is

$$D = N_{DR} + N_{RD} = 2N_{DR} \qquad \text{Q.E.D.} \tag{28}$$

and so the correlation of political views is congruent (mod 4) to the size of either group:

$$\begin{aligned} C_a &= A - D \\ &= L - 4N_{DR} \end{aligned} \tag{29}$$

Thus,

$$C_a(\tau) \equiv L \pmod 4 \tag{30}$$

as stated.

Consequence II—Denote by N_+ the number of (+1)'s in each period, and similarly, for N_-. Then,

$$\sum_{\tau=1}^{L} C_a(\tau) = L + M(L-1) \tag{31}$$

$$= \sum_{\tau=1}^{L} \sum_{k=1}^{L} a_k \, a_{k+}$$

$$= \left[\sum_{k=1}^{L} a_k \right]^2$$

$$\boxed{L + M(L-1) = (N_+ - N_-)^2} \qquad \text{(ref 23)} \tag{32}$$

Combining this with

$$N_+ + N_- = L \tag{33}$$

we obtain

$$N_\pm = (L \pm \sqrt{L + M(L-1)})/2 \tag{34}$$

where the signs may be taken in either order. M is invariant under $a_k \rightarrow (-a_k)$. Also, since $(L + M(L-1))$ must be a square,

$$M \geq \frac{-L}{L-1} \tag{35}$$

and hence, for $L > 2$

$$M \geq -1 \tag{36}$$

For $M = -1$,

$$N_+ = N_- \pm 1 \tag{37}$$

These are the binary sequences most widely used for modulation. The fact that this disparity of one between N_+ and N_- is the smallest attainable for a two-level sequence with $L \geq 2$ follows from equation (34). As a result, no balanced sequence ($N_+ = N_-$) with period greater than two can be two-level; in particular, no de Bruijn sequence except (+-) is two level.

Consequence III—If a two-level sequence is sampled every q digits, where q is prime to L, the sequence so produced is also two-level with the same levels L and M (ref 15). This can be seen by sampling the autocorrelation summation of the original sequence at the same rate, for each value of τ.

Consequence IV--The corresponding sequence of ($b_k = 0$ or 1) also has two-level autocorrelation:

$$C_a(\tau) = \sum_{k=1}^{L} (1 - 2b_k)\,(1 - 2b_{k+\tau}) \tag{38}$$
$$= 4C_b(\tau) + N_+ - 3N_-$$

$$C_b(\tau) = \begin{cases} N_- & , \quad \tau = 0 \\ (M + 3N_- - N_+)/4 & , \quad \tau \neq 0 \end{cases} \tag{39}$$

Each run of r "ones" contributes r to $C_b(0)$; it contributes (r-1) to $C_b(1)$. Hence the number of runs of (1)'s in each period is

$$C_b(0) - C_b(1) = N_- - (M + 3N_- - N_+)/4 \tag{40}$$

$$= (L - M)/4$$

and this must also be the number of runs of (0)'s, since the two kinds alternate.[1] Each run of ($r > 1$) "ones" contributes ($r - 2$) to $C_b(2)$, and each run of a single "one" contributes zero, with the exception that at each run of a single zero, there is an extra contribution of one. If the number of runs of a single zero is denoted by ${}^0B_1$ and of a single one by ${}^1B_1$,

$$C_b(0) - C_b(2) = 2((L - M)/4 - {}^1B_1) + 1 \cdot {}^1B_1 - {}^0B_1 \tag{41}$$

$${}^0B_1 + {}^1B_1 = (L - M)/4 \tag{42}$$

i.e., half of the total number of runs of symbols of either kind are of length one. Hence P4 guarantees the first clause of P2. No such simple statement is possible about the other clauses of P2.

Consequence V—It is sometimes necessary to know the number of ordered pairs of each kind of (a_k $a_{k+\tau}$) appearing in the $C_a(\tau)$ summation. Denote these by N_{++}, N_{+-}, N_{-+}, and N_{--}, and let

$$m = (M + 3N_- - N_+)/4 \tag{43}$$

Applying the reasoning of the political example to C_b,

$$\begin{aligned} N_{--} &= m \\ N_{+-} &= N_{-+} = N_- - m \\ N_{++} &= N_+ - (N_- - m). \end{aligned} \tag{44}$$

Consequence VI—The autocorrelation function of a two-level sequence is the same as that of a periodic rectangular pulse train except for a possible change in d-c level. By the Wiener-Khintchine Theorem, the power spectrum must therefore be the same also. It is a line spectrum with envelope ($\sin^2 x/x^2$), and there is a d-c value appropriate to the particular value of M.

If a sequence is used to phase-modulate a carrier, the spectrum will be the convolution of the sequence spectrum and the

[1] The average run length $2L/(L - M)$ is equal to two (the value for a random sequence) only if M is zero.

carrier spectrum. This will be free of peaks (and thereby facilitate hiding) provided the sequence has a small d-c level. Hence for the purpose of hiding, the choice of M = -1 is optimum, since it yields the most nearly balanced sequence.

In most systems built to date, the sequence period is kept less than the least expected Doppler period, in order that only the region of the (τ,ϕ) plane near the τ axis is accessible to signals. In such a case, the optimum choice of M to keep $|x|$ small off-peak would be M = 0. There is exactly one such sequence known (+++-) (its inversions and/or rotations are not considered to be independent). There is no known proof that longer sequences with M = 0 do not exist, but some restrictions can be put on the possible periods. From equations (32, 33), it follows that the period L must be an even square:

$$L = 4n^2 \qquad n = 1, 2, 3, \cdots \tag{45}$$

Turyn has shown further that n may not be a power of a single prime: $n \neq p^m$, p prime. The smallest values of L remaining are 144 and 400 (n = 6 and 10, respectively).

An additional relation for two-level sequences is derived in Appendix A.

4.4 Shift-Register Generators

4.4.1 General Logic (ref 23)

A shift-register generator (SRG), of degree n consists of n flip-flops, a clock pulse-generator, and a logic circuit, as shown in figure 4. For each flip-flop, "off" is symbolized by

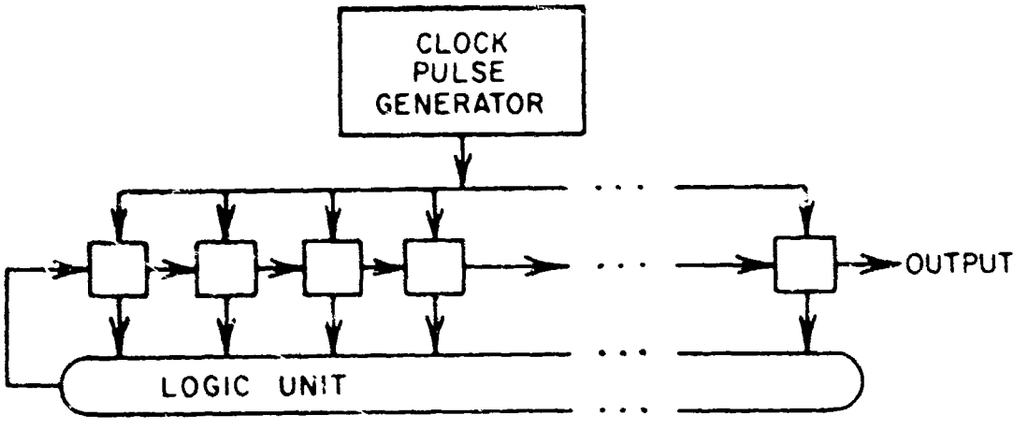


Figure 4. The general SRG.

(0) and "on" by (1). When the clock pulses arrive, the contents of each flip-flop are transferred to the next stage, as shown. The new state of the first stage is an arbitrary Boolean function of the previous contents of the register. The function specifies a (0) or (1) as desired for each of the 2^n states of the SRG; hence, there are

$$2^{2^n}$$

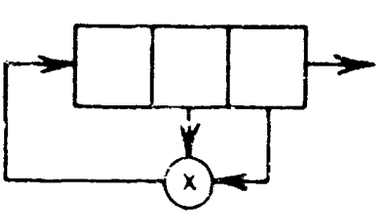
different such functions.

If the logic is correctly chosen, the SRG may produce a long sequence. The longest possible SRG sequences, for a given n, are the de Bruijn sequences ($L = 2^n$); it has been shown that there are

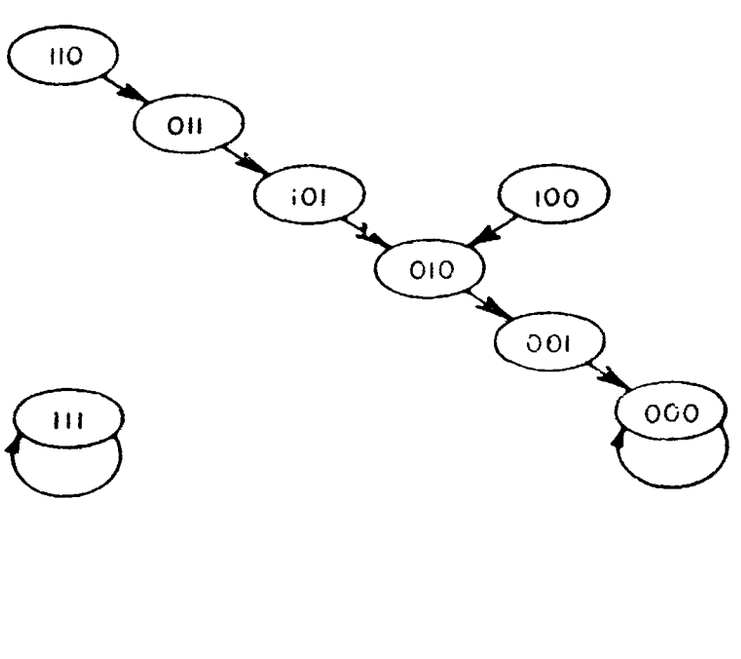
$$2^{2^{n-1}-1}$$

different de Bruijn sequences of degree n. As previously noted, none of them are two-level if $n > 1$.

The logic uniquely specifies the successor to every state of an SRG. But although each state has a unique successor, it is possible for a state to have either zero, one, or two predecessors. For example, consider a 3-stage SRG for which the new state of the first stage is the ordinary arithmetic product of the previous states of the last two stages:



The sequences of states for this register are

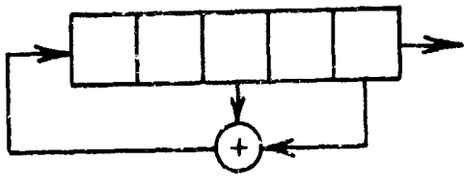


Here, (110) and (100) have no predecessors; (010) and (000) each have two predecessors. We will return to the general SRG later.

4.4.2 Linear Logic and M-Sequences (ref 12, 14, 15, 17, 18)

An important subclass of SRG's consists of those linear logic. A linear logic unit is one which computes the sum mod 2 of the contents of whichever stages feed the unit. It can easily be shown that every state of a linear SRG has a unique predecessor, and, as a result, the SRG decomposes the space of 2^n states into a number of closed cycles. Since the sum mod 2 of any number of zeroes is zero, the "all-zeroes" state always forms a separate cycle. If the stages that are to be tapped are chosen correctly, there is only one other cycle, of period (2^n-1).

Consider a (3,5) linear SRG, which is one such "linear-maximal" (or "linmax") SRG:



If the initial contents are 00001, the contents after successive clock pulses will be

(initial contents)	1) 00001
	2) 10000
	3) 01000
	4) 00100
	5) 10010
	6) 01001
	7) 10100
	8) 11010
	9) 01101
	10) 00110
	etc.
	28) 10101
	29) 01010
	30) 00101
	31) 00010
1 =	32) 00001

The sequence appearing at the output is

...1000010010110011111000110111010...

If one (0) were added to the run of four (0)'s the sequence would be a de Bruijn sequence. Hence, this SRG sequence almost satisfies

P1, P2, and P3 exactly, as it stands. But most important, it has a two-level autocorrelation:

$$C_a(\tau) = \begin{cases} 31 = L, & \tau = 0 \\ -1, & \tau \neq 0 \end{cases} \tag{46}$$

It is not difficult to prove that every linear-maximal sequence (called m-sequence) has a similar autocorrelation. In the first place, a linear logic satisfies superposition: if two identical linear SRG's A and B have arbitrary contents, and a third identical SRG C contains the sum (mod 2) of the contents of A and B, then the output digit from C will be the sum (mod 2) of the outputs of A and B. From this there follows an important

> Shift-and-add property—If an m-sequence is shifted by τ digits (τ neither zero nor a multiple of L) and added to the unshifted sequence mod 2, the sum sequence is the same sequence shifted by some other number of digits τ', e.g., for the (3,5) sequence and $\tau = 2$,
>
> ...1000010010110011111000110111010 10...
> ...1000010010110011111000110111010...
> ...1001011001111100011011101010000
> $\tau' = 28$

The dependence of τ' on τ is erratic as may be seen from the sample sequence:

τ :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
τ' :	14	38	5	25	3	10	16	19	24	6	23	20	30	1	22

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
7	18	17	8	12	27	15	11	9	4	29	21	2	26	13

This dependence is not given completely by any known function; its known properties are stated in Appendix B.

Since a (0) occurs in the sum sequence above if and only if the digits in the addend sequences agree, and since there is one more (1) than (0) in a period of an m-sequence, the autocorrelation function must be

$$C_a(\tau) = \begin{cases} L, & \tau = 0 \\ -1, & \tau \neq 0 \end{cases} \tag{47}$$

as we set out to prove.

Nothing above guarantees the existence of m-sequences, but it has been shown (ref 15, 18) that there are in fact $(\phi(2^n-1))/n$ m-sequences of degree n. (ϕ is Euler's function: $\phi(k)$ is the number of integers less than k which are prime to k, including 1.) To find the logic (i.e., which stages are tapped) of these linmax SRG's is to find the primitive irreducible polynomials over the Galois field of two elements. This computational problem has been solved with a digital computer for all linmax SRG's with n not greater than 16, and for some SRG's of each n up to 34, and the results are listed in Appendix C of reference 20. Among these permissible tap combinations are (1,2), (2,3), (3,4), (3,5), (5,6), (4,7), (4,5,6,8), (5,9), (7,10), (9,11), (6,8,11,12), ..., (20,33), (7,32,33,34). A few longer linmax SRG's are known, e.g.,

$$(136,127),\ 1,7,15,8091),\ldots(2^{127}-2,\ 2^{127}-1).$$

Given one linmax SRG of degree n, all others of degree n may be found from the Prime Sampling Theorem previously stated, which in this case at least, turns out to be exhaustive. The output is sampled every qth digit, where q is odd and prime to L. As soon as (2n-1) digits have been so produced, the SRG that will produce this new sequence can be constructed by solving n linear equations for the tap positions. Repeating the process produces all linmax SRG's of degree n (ref 17).

Another property of m-sequences that has been put to use in FM systems (ref 25, fig. 5) is that

$$\bigoplus_{k=1}^{i} b_k = b_{i+s} \quad \text{(or } (1 + b_{i+s}) \text{ depending on the choice of origin } k=1) \tag{48}$$

where the summation is mod 2, and where s is fixed for a given sequence. It can easily be shown that this property is true, and that s is equal to the number of digits separating the beginning of the run of n ones from the beginning of the run of (n-1) zeroes.

The sequence of a linmax SRG can be obtained with any desired delay by adding (mod 2) the contents of some combination of the n stages (ref 35). This could obviously be very useful in a radar system, in order to produce reference signals with different delays.

4.5 Other Sequences with M = -1

There are two other known classes of sequences with M = -1, known as "Perron" (or "Legendre" or "quadratic-residue") sequences (ref 15, 26, 36) and "twin-prime" sequences (ref 26, 39), respectively.

Perron sequences are of period (4m-1) when this quantity is a prime. Their construction is illustrated by the case for m = 3. The residues of the squares of successive integers modulo (4(3)-1 = 11) are

0, 1, 4, 9, 16(mod 11) = 5, 25(mod 11) = 3, 3, 5, 9, 4, 1, 0, 1, 4,...

and the sequence is defined by

$$a_k = \begin{cases} +1 & \text{if k is among 0, 1, 3, 4, 5 9} \\ -1 & \text{otherwise,} \end{cases} \qquad (49)$$

i.e.,

$$+ + - + + + - - - + - \quad .$$

Except for m = 1 or 2, these sequences are not m-sequences and do not have the shift-and-add property. This is an advantage in certain respects, as will be seen later.

Any periodic sequence can be generated by some SRG, and in a physical system this is often the method most economical of components. The above sequence could be generated by any one of a number of non-linear SRG's of n = 5 stages. (Four would be too few because + - + + occurs twice.) However, the sequence does not contain 21 of the 32 possible quintuplets of (+)'s and (-)'s. If an SRG were used which decomposed the set of all quintuplets into several closed cycles (as any linear SRG must, for example), it would have to be started with one of the eleven legitimate quintuplets, and if an error occurred might jump into an incorrect cycle composed of some of the 21 "bad" quintuplets. As previously noted, non-linear SRG's need not generate closed cycles. This fact can be used to generate; e.g., Perron sequences with a non-linear SRG which avoids the above two difficulties, with each illegitimate state (here, one of the 21 bad quintuplets) leading back into the cycle of legitimate states.

The twin-prime sequences have period L = p(p+2) where p and (p+2) are both prime, and are formed by a method similar to that for Perron sequences. The twin-prime sequence for p = 3 is the same as the (1,4) m-sequence. The p=5 sequence in b_k notation is

10111000111110111001000010101100100

The remarks on the generation of Perron sequences apply also to twin-prime sequences, of course.

4.6 Acquirable Codes

To locate a given target in range by testing every integral value of τ would require L tests. However, only $\log_2$ L tests would be needed if the target could be localized to within 1/2 L, then to within 1/4 L, etc. The best practical solution to date is to use certain sequences obtained by combining shorter sequences with relatively prime periods, so that

$$L = p_1 \, p_2 \cdots p_k \tag{50}$$

where p_i is the period of the i^{th} subsequence. For these codes, at most

$$N = p_1 + p_2 + \cdots + p_k \tag{51}$$

tests are needed, and on the average, only N/2. These codes have been used in the Goldstone deep-space ranging system (ref 1, 49).

4.7 The Ambiguity Function for Sequences

If the period of the modulation waveform is not kept small in comparison with a Doppler cycle, the output of a correlator is given not by the autocorrelation function but by the full ambiguity function.

The squared magnitude of the ambiguity function for sequences is defined analogously to that for continuous functions:

$$C_{\tau s} = \left| \sum_n a_n \, a_{n+\tau} \, u^{ns} \right|^2 \tag{52}$$

where

$$u = \exp(2\pi i/L) \tag{53}$$

This is obviously equal to L^2 at the origin and is zero elsewhere along the Doppler frequency (s) axis. Lerner (ref 21) has computed $C_{\tau s}$ for m-sequences and found

$$\begin{aligned} C_{\tau s} &= L^2 \quad , \quad \tau, s \equiv 0, 0 \pmod L \\ &= 0 \quad , \quad \tau \equiv 0 \pmod L, \; s \not\equiv 0 \pmod L \\ &= 1 \quad , \quad \tau \not\equiv 0 \pmod L, \; s \equiv 0 \pmod L \\ &= L + 1 \quad , \quad \text{elsewhere} \end{aligned} \tag{54}$$

i.e., a peak at the origin and a plateau elsewhere cut by valleys along the axes. This calculation uses the shift-and-add property of m-sequences; other (e.g., Perron) sequences with two-level autocorrelation functions, but not having the shift-and-add property do not in fact exhibit the same peak-free plateaus.

It can be shown that

$$\sum_{\tau, s} C_{\tau s} = L^3 \tag{55}$$

and hence, this ambiguity function is very nearly the smoothest obtainable, i.e., has the smallest maximum value off-peak; the only further smoothing possible would be the lowering of the plateau height from (L + 1) to L by sacrificing the valley along the τ-axis

$$\begin{aligned} C_{\tau s} &= L^2 \quad , \tau,s \neq 0,0 \\ &= 0 \quad , \text{elsewhere on the s-axis (necessary)} \\ &= L \quad , \text{at the other } (L^2 - L) \text{ points} \end{aligned} \tag{56}$$

This requires that

$$M = \sqrt{L} \tag{57}$$

and from equation (A-26),

$$\begin{aligned} (N_+ - N_-)^2 &= L + M(L - 1) \\ &= n^2 + n(n^2 - 1) \end{aligned} \tag{58}$$

i.e., $(n^3 + n^2 - n)$ must be a perfect square. This is never the case for $1 < n \leq 200$, at least; and hence, there are no such "smoothest-possible" sequences for $L \leq 40{,}000$.

Since moving off the τ axis implies a degradation of the normalized ambiguity function magnitude from $1/L$ to $\sqrt{L + 1} / L \approx 1/\sqrt{L}$ for an m-sequence, it is clearly advantageous to keep the integration time (Lt_o) much less than one Doppler cycle. If the integrator is a filter instead of some type of block integrator (one which computes $\sum_1^1 a_k \, a_{k+\tau}$ exactly) however, the output off-peak may be degraded in two ways. First, the infinite tail of the filter impulse response will "remember" some input contributions extending back over past Doppler cycles. By using a short time constant, this may be made as small as desired. But then the second effect appears: the off-peak autocorrelation is only constant if the integration is a block integration extending over an integral number of sequence periods. Thus, the output of a filter will fluctuate appreciably unless the time constant is much longer than the sequence period. (This effect is investigated in Appendix C.) Since the normalized off-peak autocorrelation ($-1/L$ for an m-sequence) becomes better with increasing sequence period L, it is all the more important that the bit time (t_o) be short.

5. BLOCK DIAGRAM OF A SYSTEM

Craig, Fishbein, and Rittenbach have described several systems that use m-sequence modulation (ref 24, 25, 73). Without specifying the particular kind of modulation, consider the following system:

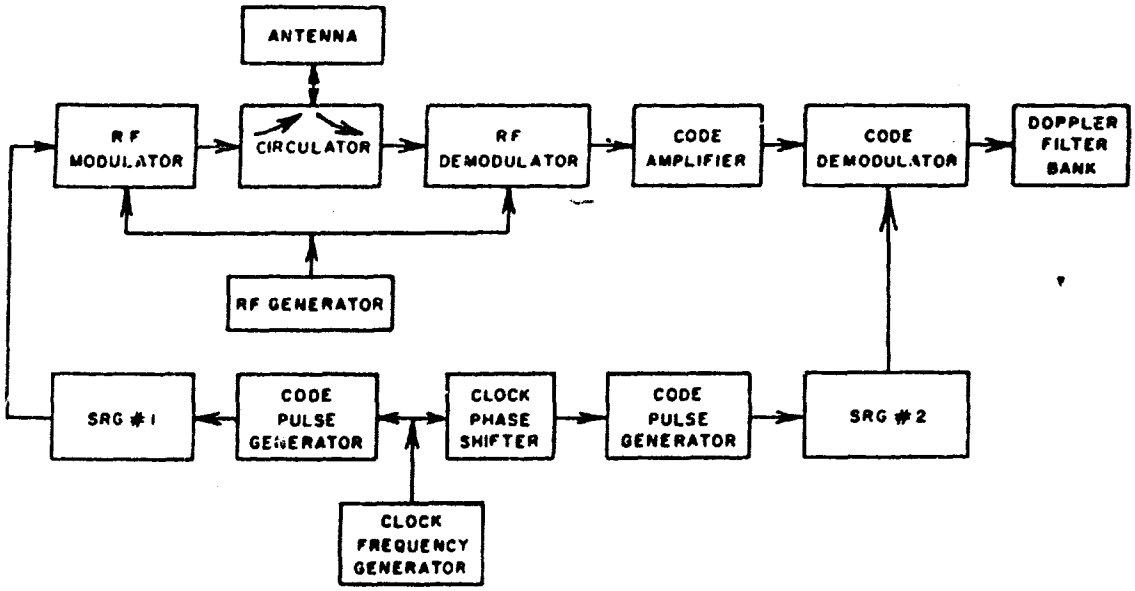


Figure 5. Block diagram of a system.

Each rotation of the continuously variable phase-shifter causes SRG 2 to drop one digit further behind SRG 1 in the m-sequence. The output of the RF demodulator is a Doppler signal chopped by the m-sequence, and hence, consists of components too high in frequency to pass any of the filters, which serve as the integrators. When the reference code from SRG 2 has the correct delay, the code demodulator reassembles the chopped Doppler into an unchopped wave, which passes some filter. Range is measured by the number of digits SRG 2 has to drop behind SRG 1 to produce a peak in the output of some filter.

The system can be altered in certain ways to utilize transmitter leakage as the local oscillator. Unlike the above system, this alteration requires a sequence with the shift-and-add property. This version has been implemented by Craig et al using FM and 5-stage linmax SRG's (L = 31). They report "an over-all receiver sensitivity of -140 dbm on slowly moving targets." Since the system must search serially in range, the acquisition time will be comparatively large.

6. NON-BINARY CODES FOR CW

If the number of modulation states is greater than two, the multiplication operation and the autocorrelation function must be

redefined. If 0, 120, and 240 deg PM is us the natural representation of the a_k consists of the cube roots oi unity, and

$$C_a(\tau) = \sum_k a_k^* a_{k+\tau} \tag{59}$$

In general, q states of equiangular PM are represented by the qth roots of unity and this autocorrelation is the natural one.

One class of perfect codes is known, of period q^2, for any q (ref 50). One period of one of these codes consists of the following powers of s ($s = \exp(2\pi i/q)$):

$$1,2,3,\ \ldots\ q,\ 2,4,6,\ldots,\ 2q,\ 3,6,9\ldots.\ 3q,\ldots\ldots,q,2q,3q,\ldots,q^2$$

For q = 3 this is the sequence

$$s,s^2,1,s^2,s,1,1,1,1$$

The autocorrelation function is

$$C_a(\tau) = \begin{cases} L = q^2, & \tau = 0 \\ 0, & \tau \neq 0 \end{cases} \tag{60}$$

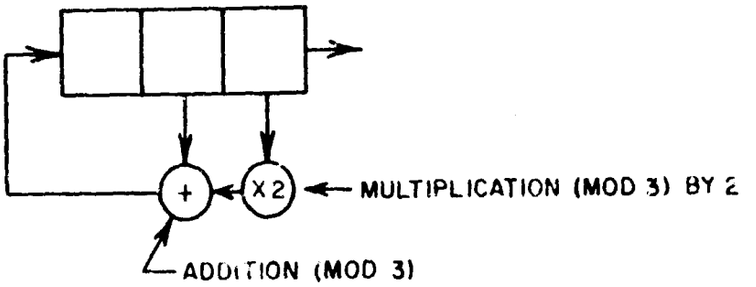
The limitation on length, given q, is a serious disadvantage of these sequences. Sequences of any desired length but with a poorer autocorrelation can be obtained from multi-state SRG's. Here q may be any power of a prime,

$$q = p^m, \tag{61}$$

and linear SRG's are those which have a logic consisting of multiplication by 0,1,2,..., or (q-1) at each tap, followed by addition mod q. As before there exist linmax SRG's of every length n with autocorrelation

$$C_a(\tau) = \begin{cases} L = q^n - 1, & \tau = 0 \\ -1, & \tau \neq 0 \end{cases} \tag{62}$$

Under addition mod q, these sequences have the shift-and-add property. Connections for some linmax SRG's are given by the coefficients of the primitive irreducible polynomials in references 19 and 41; e.g., for q = 3, reference 19 gives $(x^3 - x - 2)$ as a primitive irreducible polynomial. The coefficients are 1,0,-1,-2, and the last three specify a linmax SRG:



The m-sequence produced is ...0010121120111002021221022 2...

If, on the other hand, the modulation states are "off," "on," 0 deg , and "on" 180 deg, the natural representation is $a_k = 0$, +1, -1. Tompkins (ref 45) has found all of the perfect codes of this kind for $L \leq 19$ by trial. For $L > 13$, these have few non-zero terms, a distinct drawback, since the average power suffers accordingly.

Non-binary sequences have not yet been used in radar systems to the author's knowledge.

ACKNOWLEDGMENT

The author is indebted to Mr. R. T. Fitzgerald for first introducing him to the subject, and for many stimulating and enlightening discussions.

7. REFERENCES AND BIBLIOGRAPHY

(1) Notes from special summer session on Modern Radar Techniques, Moore School of Electrical Engineering, U. of Pa., (June 1961); in particular, H. Urkowitz on "Ambiguity and Resolution"; M. P. Ristenbatt on "Pseudo-Random Sequences."

(2) Woodward, P. M., Probability and Information Theory, with Applications to Radar, (McGraw-Hill Book Co., 1953).

(3) Siebert, W. M., "A Radar Detection Philosophy," IRE Transactions on Information Theory, Vol. IT-2, #3, (Sept. 1956) pp. 204-221

(4) Turin, G. L., "A Review of Correlation, Matched-Filter, and Signal-Coding Techniques, with Emphasis on Radar Applications," Hughes Aircraft Co., TM 559 (April 1957) Vol I and Vol II (Confidential).

(5) Horton, B. M., "Noise-Modulated Distance Measuring Systems," Proc. of the IRE, Vol 47 (1959), pp. 821-828.

(6) Feller, W., "An Introduction to Probability Theory and Its Applications," second edition, (Wiley, 1957).

(7) Klauder, J. R., "The Design of Radar Signals Having Both High Range Resolutions and High Velocity Resolution," Bell Systems Technical Journal, vol 39, (July 1960), pp. 809-820.

(8) Allen, J. L., "A Quantitative Examination of the Radar Resolution Problem," M.I.T. Lincoln Laboratory TR 281 (Sept. 1962).

(9) Martin, M. H., "A Problem in Arrangements," Bulletin of the American Math. Society, Vol. 40, (Dec 1934), pp. 859-864.

The original paper on "de Bruijn" sequences. Similar material can be found in ref 52 and, without proof, in Karl Popper's "The Logic of Scientific Discovery."

(10) de Bruijn, N. G., "A Combinatorial Problem," Koninklijke Nederlandse Akademic van Wetenschappen, Proceedings, Vol. 49 (part 2), (1946), pp. 758-764.

Nonconstructive enumeration of de Bruijn sequences.

(11) Good, I. J., "Normal Recurring Decimals," Journal of the London Math. Society, Vol. 21, part 3, (July 1946), pp. 167-169.

(12) Rees, D., "Note on a Paper by I. J. Good, Ref 11, pp. 167-169. This is the first paper on m-sequences, both binary and higher base. Does not consider the autocorrelation.

(13) Stein, S. K., "The Mathematician as Explorer," Scientific American, Vol. 205, (May 1961), pp. 148-158.

On de Bruijn sequences. See letters in the July 1961 issue.

(14) Gilbert, E. N., "Quasi-Random Binary Sequences," Bell Telephone Laboratories Memorandum, MM-53-1400-42, Case 38718 (Nov. 27, 1953).

Considers two-tap linmax SRG's.

(15) Golomb, S. W., "Sequences with Randomness Properties," Glenn L. Martin Co., Baltimore, Md., Terminal Progress Report (14 June 1955).

Readable introduction to linear SRG's and Perron sequences.

(16) Elspas, B., "A Radar System Based on Statistical Estimation and Resolution Considerations," Stanford Electronics Laboratories TR-361-1, (1 August 1955), AD 207896.

Considers correlation theory, m-sequences, systems components, etc. The conjecture on p. 139 is false.

(17) Birdsall, T. G., and Ristenbatt, M. P., "Introduction to Linear Shift-Register Generated Sequences," University of Michigan Research Institute TR-90, (October 1958), AD 205380.

Perhaps the best elementary introduction to m-sequences.

(18) Zierler, N., "Linear Recurring Sequences," Journal of the Soc. Indust. Appl. Math., Vol. 7, (March 1959), pp. 31-48.

Rigorous exposition of m-sequences, including autocorrelation.

(19) Albert, A. A.,"Fundamental Concepts of Higher Algebra," (University of Chicago Press, 1956).

The best reference for the basic algebra of m-sequences.

(20) Peterson, W. W., "Error-Correcting Codes," (Wiley, 1961).

Another good reference on algebra. Covers SRG's and m-sequences from the standpoint of error correction.

(21) Lerner, R. M., "Signals with Uniform Ambiguity Functions," IRE Convention Record, part 4, (1958), pp 27-36.

The only reference on the theory of sequence ambiguity functions.

(22) Titsworth, R. C., and Welch, L. R., "Modulation by Random and Pseudo-Random Sequences," Jet Propulsion Laboratory of Calif. Inst. of Technology (JPL), PR 20-387, (12 June 1959), AD 225596.

Investigation of spectra.

(23) Golomb, S. W., and Welch, L. R., "Nonlinear Shift-Register Sequences," JPL Memo. 20-149, (25 Oct. 1957), AD 159888.

Classic exposition; theoretical and experimental sections.

(24) Fishbein, W., and Rittenbach, O. E., "Correlation Radar Using Pseudo-Random Modulation," IRE Convention Record, Part 5 (1961), pp. 259-277.

(25) Craig, S. E., Fishbein, W., and Rittenbach, O. E., "Continuous-Wave Radar with High Range Resolution and Unambiguous Velocity Determination," IRE Transactions on Military Electronics, Vol. 6, (April 1962), pp. 153-161.

(26) Baumert, L., Easterling, M., Golomb, S. W., Viterbi, A., "Coding Theory and Its Applications to Communications," JPL TR 32-67, (31 March 1961), AD 257752.

Section II, "Codes with Special Correlation," collects a great variety of material. Section III covers "A Pseudo-Random Coded Ranging System."

(27) Siebert, W. M., "Studies of Woodward's Uncertainty Function," M.I.T. Electronics Research Laboratory, Quarterly Progress Report, (15 April 1958), AD 208249, pp 90-94.

(28) Sussman, S. M., "Least-Square Synthesis of Radar Ambiguity Functions," IRE Transactions on Information Theory, Vol. 8, (April 1962), pp. 246-254.

(29) Wilcox, C. H., "The Synthesis Problem for Radar Ambiguity Functions," University of Wisconsin Mathematics Research Center, Tech. Summary Report No. 157, (April 1960).

(30) Klauder, J. R., Price, A. C., Darlington, S., and Albershein, W.J., "The Theory and Design of Chirp Radars," Bell System Technical Journal, Vol. 39, (July 1960), pp. 745-808.

(31) Davenport, W. B., Jr., Johnson, R. A., and Middleton, D., "Statistical Errors in Measurements on Random Time Functions," Journal of Applied Physics, Vol. 23, (April 1952), pp. 377-388.

(32) Lytle, D. W., "Experimental Study of Tapped Delay-Line Filters," Stanford Electronics Laboratories TR 361-3, (30 July 1956), AD 105406.

(33) Turyn, R., and Storer, J., "On Binary Sequences," Proceedings of the Am. Math. Soc., Vol. 13, (1962), p. 394.

(34) Zierler, N., "Several Binary-Sequence Generators," M.I.T. Lincoln Laboratory TR 95, (12 Sept 1955), AD 89135.

(35) Curry, R. C., "A Method of Obtaining Arbitrary Phases of an m-Sequence," University of Rochester Electrical Engineering Dept., (1 Nov. 1960), Ad 248455.

(36) Perron, I., "Bermerkungen uber die Verteilung der quadratischen Reste," Math. Zeitschrift, Vol. 56, (1952), pp. 122-130.

(37) Paley, R. E. A. C., "On Orthogonal Matrices," Journal of Math. and Physics, Vol. 12 (1933), pp. 311-320.

(38) Hall, M., Jr., "A Survey of Difference Sets," Proceedings of the Am. Math. Soc., Vol 7, (1956), pp. 975-986.

(39) Brauer, A., "On a New Class of Hadamard Determinants," Math. Zeitschrift, Vol. 58, (1953), pp. 219-225.

(40) Bussey, W. H., "Galois Field Tables," Bulletin of the Am. Math. Soc., Vol. 12, (1905), pp. 22-38; Vol. 16, (1909), pp. 188-206.

(41) Titsworth, R. C., "Correlation Properties of Cyclic Sequences," thesis, Calif. Inst. of Technology, (1962).

(42) Turyn, R., " Optimal Codes Study, Final Report," Sylvania Applied Research Laboratories (29 Jan. 1960), AD 236122.

(43) Golomb, S. W., Welch, L. R., and Goldstein, R. M., "Cycles from Nonlinear Shift Registers," JPL PR 20-389, (31 Aug. 1959), AD 230533.

(44) Heimiller, R. C., "Phase Shift Pulse Codes with Good Periodic Correlation Properties," IRE Transactions on Information Theory, Vol. 7 (Oct. 1961), pp. 254-257.

(45) Tompkins, D. N., "Codes with Zero Correlation," Hughes Aircraft Co., Culver City, Calif., TM 651, 251 pp

(46) Victor, W. K., Stevens, R., and Golomb, S. W., "Radar Exploration of Venus," JPL TR 32-132, (1 Aug 1961), AD 263012.

(47) Other unclassified ASTIA reports on specialized aspects of codes include AD 236397, 236796, 239172, 241518, 241519, 242047, 250212.

(48) "Communication Techniques—Deep Space Range Measurement," JPL Research Summary No. 36-1, Vol. 1, (15 Feb. 1960), pp. 39-46.

(49) DeLong, D.F., Jr., "Three-Phase Codes," Lincoln Lab Group Report 47-28, (1959).

(50) Frank, R. L., Zadoff, S. A, Heimiller, R. C., "Phase-Shift Codes with Good Periodic Correlation Properties," IRE Transactions on Information Theory, Vol 8, (Oct 1962), pp. 381-382.

(51) Frank, R. L., "Polyphase Codes with Good Nonperiodic Correlation Properties," IRE Transactions on Information Theory, Vol. 9, (Jan. 1963), pp. 43-45.

(52) Ford, L. R., Jr., "A Cyclic Arrangement of n-tuples," Rand Corp. p-1070, (1957).

(53) Welti, G., "Quarternary Codes for Pulsed Radar," IRE Transactions on Information Theory, Vol. 6, (June 1960), pp 400-408.

(54) Turyn, R., "Ambiguity Functions of Complementary Sequences," IRE Transactions on Information Theory, Vol. 9, (Jan. 1963), pp. 46-47.

(55) Price, R. et al, "Radar Echoes from Venus," Science, Vol. 129. (20 March 1959), pp. 751-753.

(56) Easterling, "Long Range Precision Ranging System," JPL Report No. 32-80, (1961) AD 261178.

(57) Easterling, JPL Research Summary 36-7, Vol 1, (1961).

(58) Golomb, S. W., "Structural Properties of Pseudo-Noise Sequences," JPL Section Report 8-574 (1958)

(59) Golomb, S. W., "Sequences with the Cycle-and-Add Property," JPL Section Report 8-573 (1957).

Introductory Readings on Various Aspects

Correlation theory - References 1, 2, 3, 4, 8.
Applications of correlation theory - References 3, 4, 5, 7, 16.
Linear SRG's and M-Sequences - References 1, 15, 16, 17.
Linear SRG's, rigorously treated - References 12, 15, 18, 20, 34.
Nonlinear SRG's - References 23, 43.
Perron sequences - References 15, 36.
deBruijn sequences - References 9, 10, 11, 13, 23, 52.
Spectra of sequences - References 1, 22, and classified references.
Systems - References 16, 24, 25, 46, and classified references.
Acquirable codes - References 1, 48.
Multi-state sequences - References 44, 45, 49, 50.

APPENDIX A. MESH RELATIONS FOR SEQUENCES WITH TWO-LEVEL AUTOCORRELATION

Let ($a_k = \pm 1$) be a sequence of period L with a two level periodic autocorrelation. If q is a factor of L, then the sequence can be divided into q "meshes" by sampling every qth digit beginning with any of the first q digits. We will derive relations between the sums S_{qi} of the digits in the various such meshes:

$$S_{qi} = \sum_{k} a_k \quad , \quad k \equiv i \pmod{q} \tag{A-1}$$

One tool with which such a separation into meshes can be accomplished is $\exp(2\pi i\tau/q)$:

$$\sum_{\tau=1}^{L} C(\tau) \exp(2\pi i\tau/q) = L \cdot 1 + M \sum_{\tau=1}^{L-1} \exp(2\pi i\tau/q) \tag{A-2}$$

$$= \begin{cases} L + M(L \cdot 1), & q = 1 \\ L - M, & q > 1 \end{cases}$$

But also,

$$\sum_{\tau=1} C(\tau) \exp(2\pi i\tau/q) = \sum_{\tau=1}^{L} \sum_{k=1}^{L} a_k a_{k+\tau} \exp(2\pi i\tau/q) \tag{A-3}$$

$$= \sum_{k=1}^{L} a_k \exp(-2\pi ik/q) \sum_{\tau=1}^{L} a_{k+\tau} \exp(2\pi i(k+\tau)/q)$$

$$= \sum_{k} a_k \exp(-2\pi ik/q) \sum_{\tau} a_\tau \exp(+2\pi i\tau/q)$$

$$= \left[\sum_k a_k \cos(2\pi k/q) - i \sum_k a_k \sin(2\pi k)/q)\right]\left[\sum_k a_k \cos(2\pi k/q) + i \sum_k a_k \sin(2\pi k/q)\right]$$

$$L + M(L \cdot \delta_{q,1} - 1) = \left[\sum_k a_k \cos(2\pi k/q)\right]^2 + \left[\sum_k a_k \sin(2\pi k/q)\right]^2 \tag{A-4}$$

where δ is the Kronecker delta.

We now specialize this temporarily to the case M = 0. These sequences, which were described in section 4.3 have periods of the form

$$L = 4n^2 \quad , \quad n = 1, 2, 3, \ldots \quad , \quad n \neq p^m, \ p \text{ prime} \tag{A-5}$$

Hence L is always divisible at least by 2, 4, n, and n^2.

For q = 2, the mesh relation above yields

$$4n^2 = (S_{22} - S_{21})^2 \tag{A-6}$$

We know also that

$$\sum_{i=1}^{q} S_{qi} = \sum_{k=1}^{L} a_k = N_+ - N_- = 2n \tag{A-7}$$

Choosing $S_{22} > S_{21}$ arbitrarily, we find that

$$S_{21} = 0 \tag{A-8}$$

and

$$S_{22} = 2n \tag{A-9}$$

i.e., the first mesh of alternate digits is balanced and the second contains the entire imbalance between N_+ and N_-.[1]

For q = 4,

$$4n^2 = (S_{44} - S_{42})^2 + (S_{41} - S_{43})^2 \tag{A-10}$$

From the case q = 2, we have

$$S_{41} + S_{43} = 0 \tag{A-11}$$

and

$$S_{42} + S_{44} = 2n. \tag{A-12}$$

Again choosing arbitrary signs and indices wherever possible,

$$-S_{43} = S_{41} = + (S_{42} \, S_{44})^{1/2} \tag{A-13}$$

and

$$S_{42} + S_{44} = 2n \tag{A-14}$$

with the auxiliary conditions that

---

[1] This was first discovered and proved by N. Karayianis and C. A. Morrison along with a number of other results concerning sequences with M = 0 that are not included here.

$$|S_{4i}| \leq n^2 \tag{A-15}$$

$$S_{42} \geq 0 \tag{A-16}$$

$$S_{4i} > 0 \tag{A-17}$$

and

$$S_{4i} \equiv n \pmod 2 \tag{A-18}$$

For any n, one solution is given by

$$-S_{43} = S_{41} = S_{42} = S_{44} = n \qquad (I) \tag{A-19}$$

for even n, there is also the solution

$$S_{41} = S_{42} = S_{43} = 0;\ S_{44} = 2n \qquad (II) \tag{A-20}$$

These are all of the solutions except for a small number of others that may be found straightforwardly by listing the squares of successive composite values of S_{41}, factoring these into S_{42} and S_{44}, and calculating $n = (S_{42} + S_{44})/2$. This is required to be an integer and to have the same parity as S_{4i}, as noted above. The only such irregular solutions for $n \leq 20$ are

$n = 10$: $S_{4i} = (8, 4, -8, 16)$ or $(6, 2, -6, 18)$

$n = 15$: $S_{4i} = (9, 3, -9, 27)$

$n = 20$: $S_{4i} = (12, 4, -12, 36)$

The others for $n \leq 40$ are for $n = 26(2), 30(2), 34(2), 35$, and $40(2)$.

Relations similar to the above can be written for each of the factors of any sequence with two-level autocorrelation. The ones above are suited to a computer search for sequences with $M = 0$. Such a search might begin by writing the admissible combinations of lengths of runs of (+1)'s and (-1)'s from the two rules governing them; e.g., for $n = 2$ these are

-1	+1
3,1,1,1	5,2,2,1
	4,3,2,1
	3,3,3,1
2,2,1,1	5,3,1,1
	4,4,1,1

where the choice has been made that

$$N_+ > N_-$$

These would then be interleaved in all possible independent ways and each of the resulting sequences tested cyclically to see if it obeys the mesh relations for all q dividing L. Any sequences surviving this test would then be tested for two-level autocorrelation, a considerably longer process.

We now return to the case of general M. For some higher values of q, the right side of the basic mesh relation has some coefficients which are irrational and mutually independent; e.g., for q = 5, after manipulation

$$L - M = \sum_{50} -2\sum_{51} + 3(S_{51}\,S_{52} + S_{53}\,S_{54})$$

$$-2c\left(\sum_{52} - 3(S_{51}\,S_{52} + S_{53}\,S_{54})\right) \qquad \text{(A-21)}$$

$$+4c^2\left(\sum_{51} -3(S_{51}\,S_{52} + S_{53}\,S_{54})\right)$$

where

$$c = \cos(2\pi/10) = \cos 36 \text{ deg}$$

and

$$\sum_{qJ} = \sum_{i=1}^{q} s_{qi}\, s_{q,i+j} \qquad \text{(A-22)}$$

Since the lowest order polynomial equation with rational coefficients satisfied by cos 36 deg is

$$8c^3 - 8c^2 + 1 = 0 \qquad \text{(A-23)}$$

c and c^2 are irrational and incommensurable, and each of the last two terms in the mesh relation must be zero. Hence

$$L - M = \sum_{50} - \sum_{51} \qquad \text{(A-24)}$$

and

$$\sum_{51} = \sum_{52} = 3(S_{51}\,S_{52} + S_{53}\,S_{54}) \qquad \text{(A-25)}$$

Using the notation given by (A-22), the mesh relations for small values of q are

$q = 1$: $L + M(L-1) = \sum_{10}$ [Eq. (32)]

$q = 2$: $L - M = \sum_{20} - \sum_{21}$ e.g. [Eq. (A-6)]

$q = 3$: $L - M = \sum_{30} - \sum_{31}$

$q = 4$: $L - M = \sum_{40} - \sum_{42}$ e.g. [Eq. (A-10)]

$q = 5$: $L - M = \sum_{50} - \sum_{51}$

$$\sum_{51} = \sum_{52} = 3\,(S_{51}\,S_{52} + S_{53}\,S_{54})$$

$q = 6$: $L - M = \sum_{60} + \sum_{61} - \sum_{62} - \sum_{63}$

$q = 8$: $L - M = \sum_{80} - \sum_{84}$

$$\sum_{81} = \sum_{83}$$

$q = 12$: $L - M = \sum_{12,0} + \sum_{12,2} - \sum_{12,4} - \sum_{12,6}$

$$\sum_{12,1} = \sum_{12,5}$$

Since no choice of signs or indices has been made here, all of these relations must be obeyed cyclically in the choice of sequence origin. The same is true of the universal auxiliary relation

$$\sum_{i=1}^{q} S_{qi} = \sum_{k=1}^{L} a_k = N_+ - N_- = (L + M(L-1))^{1/2} \qquad \text{(A-26)}$$

APPENDIX B. THE SHIFT-AND-ADD RELATIONS

If an m-sequence is shifted τ digits and added to the unshifted sequence mod 2, the result is the same sequence shifted to τ' digits. It is necessary to know the dependence of τ' on τ when designing a linmax-coded radar using the transmitter leakage for the local oscillator (ref 25), and for certain other purposes. Here we state and illustrate some relations between τ and τ' without proof; the proofs all proceed straightforwardly using the matrix theory found; e.g., in reference 17.

If a shift of τ digits in the addend sequence leads to a shift of τ' in the sum sequence, we write $\tau \rightarrow \tau'$

If

$$\tau \rightarrow \tau' \tag{B-1}$$

then

$$\tau' \rightarrow \tau$$

Hence the relation ($\rightarrow$) is reflexive and should be written ($\leftrightarrow$). As a result we will symbolize τ and τ' more symmetrically by τ_1 and τ_2.

If

$$\tau_1 \leftrightarrow \tau_2 \tag{B-2}$$

then

$$2\tau_1 \leftrightarrow 2\tau_2, \text{ both sides modulo } L = 2^n - 1.$$

If

$$\tau_1 \leftrightarrow \tau_2 \tag{B-3}$$

then

$$(-\tau_1) \leftrightarrow (\tau_2 - \tau_1), \text{ both mod } L.$$

If (T_1, T_2) describes a two-tap linmax SRG, then

$$T_1 \leftrightarrow T_2 \tag{B-4}$$

for the m-sequence generated by that SRG.

There is one other relation which permits writing the (τ, τ') dependence compactly:

If

$$\tau_1 \leftrightarrow \tau_2$$

and

$$\tau_2 - \tau_1 \leftrightarrow \tau_3$$

and

$$\tau_3 - (\tau_2 - \tau_1) \leftrightarrow \tau_4$$

then

$$\tau_4 - (\tau_3 - (\tau_2 - \tau_1) \equiv \tau_1 \pmod{L} \qquad \text{(B-5)}$$

As a result the entire dependence given in section 4.4.2 for the (3,5) m-sequence can be written as a 5 x 3 matrix (generally a $[\frac{2^n - 2}{6}]$ x 3 matrix, where $\lceil\ \rceil$ symbolizes "smallest integer not less than.")

$$\begin{bmatrix} 1 & 13 & 17 \\ 2 & 26 & 3 \\ 4 & 21 & 6 \\ 7 & 9 & 15 \\ 8 & 11 & 12 \end{bmatrix}$$

where, for example,

$$1 \leftrightarrow 1 + 13 = 14$$
$$13 \leftrightarrow 13 + 17 = 30$$
$$17 \leftrightarrow 17 + 1 = 18$$

and similarly for each row. Every integer from 1 to 30 appears exactly once either as an element or the sum of two elements in some row, the rows double as in relation (B-2) and the sum of each row is 31.

The entire matrix can be written using (B-4), which in this case reads

$$3 \leftrightarrow 5 ,$$

followed by alternate applications of relations (B-2) and (B-3). This is not true for larger n: the results of not more than (6n) shifts can be obtained this way. Here this gives all 30. For larger n or for SRG's with more than two taps, it is necessary to calculate the results of some shifts by actual addition of sequences. Relations (B-2) and (B-3) still greatly reduce the labor involved, but by a factor somewhat less than (6n), due to short cycles.

APPENDIX C: FILTER INTEGRATION OF M-SEQUENCES

We will treat a simple case: the RC integration of a mixer output when the mixer inputs are both m-sequence telegraph signals.

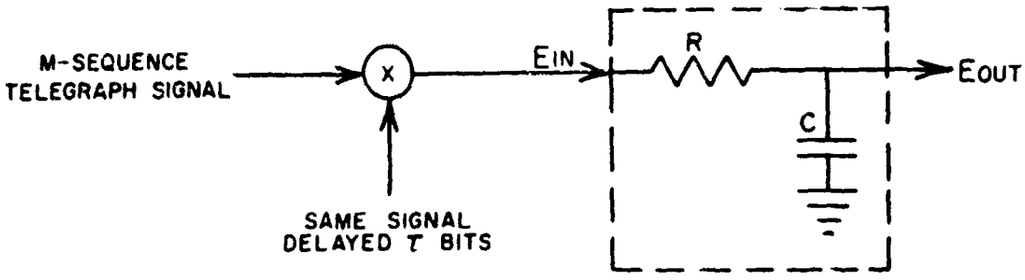


Figure C-1. Filter integration of an m-sequence.

As a function of the history of the input voltage to the integrator E_{in}, the output voltage E_{out} is

$$E_{out}(t) = K \int_{-\infty}^{t} e^{K(u-t)} E_{in}(u)\, du \qquad \text{(C-1)}$$

where

$$K = 1/RC$$

When $\tau = 0$, E_{in} is dc and E_{out} asymptotically approaches E_{in}. When τ is a non-zero integer, E_{in} is the same m-sequence according to the shift-and-add property. If the sequence is (---+-++) and the recent history of E_{in} is (·····+-++|--) then the integrand is as shown in figure C-2.

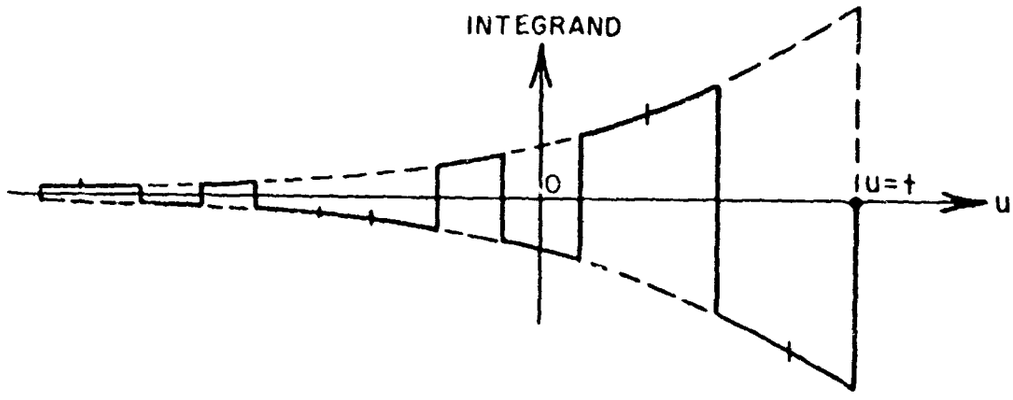


Figure C-2. Integrand of equation C1.

At the end of any bit, the integral is

$$E_{out} = (1 - e^{-Kt_o}) \sum_{n=0}^{-\infty} a_n e^{nKt_o}$$

$$= (1 - e^{-Kt_o}) \left[a_o \left(1 + e^{-LKt_o} + e^{-2LKt_o} + \cdots \right) \right.$$

$$+ a_{-1} \left(e^{-Kt_o} + e^{-(L+1)Kt_o} + \cdots \right)$$

$$\left. + a_{-L+1} \left(e^{-(L-1)Kt_o} + \cdots \right) \right] \qquad (C\text{-}2)$$

$$E_{out} = \frac{1-e^{-Kt_o}}{1-e^{-LKt_o}} \sum_{n=0}^{-L+1} a_n e^{nKt_o} \qquad (C\text{-}3)$$

Unlike the output of an L-bit block integrator (one which computes $\sum_{1}^{L} a_k a_{k+\tau}$ exactly) with the same input, this E_{out} is not constant in time. If the "recent" part of the sum is a section of the sequence containing predominantly (+)'s, the sum will be positive, etc. Expanding the exponential,

$$\sum_{0}^{-L+1} = \sum_{0}^{-L+1} a_n (1 + nKt_o + \cdots) \qquad (C\text{-}4)$$

and the first term does not fluctuate; it is just

$$\sum_{n=0}^{-L+1} a_n = -1 \qquad (C\text{-}5)$$

A crude limit on the fluctuating second term can be made by assuming that the "recent" half of the sum has all a_n equal to (-1) and the distant half (+1).

$$\sum_{0}^{-L+1} a_n \, n < - \sum_{0}^{-L/2} n + \sum_{-L/2}^{-L+1} n \qquad (C\text{-}6)$$

$$< L^2/4.$$

Doubling this quantity gives a pessimistic estimate of the peak-to-peak fluctuations of the sum in E_{out} as the "recent" part of the sequence changes back and forth between "predominantly (+)'s" and "predominantly (-)'s" as time goes by.

A much better estimate can be made by using a conjectured approximate limit on the truncated autocorrelation function of an m-sequence

$$\sum_{t=1}^{J} a_k \, a_{k+o} \lesssim (3L/2)^{1/2}, \quad J \leq L \tag{C-7}$$

Then

$$\sum n_{an} \lesssim \sum_{l-d}^{L} n - \sum_{l}^{d} n \tag{C-8}$$

where

$$d = (3L/2)^{1/2}$$

Hence

$$\sum n \, a_n \lesssim L \, (3L/2)^{1/2} \tag{C-9}$$

For Perron sequences the limit on the truncated autocorrelation seems to be much smaller.